Handel Information Technologies, Inc.

Administration Tree Training Document for RiteTrack®

Handel Information Technologies, Inc.

www.handelit.com

Administration Tree Training Document for *RiteTrack®*

Introduction:

This documentation has been created as an overview for training on the Administration Tree in the RiteTrack® System. If you have any questions after reading this and your training, feel free to contact Handel Information Technologies, Inc. at the following:

Handel Information Technologies, Inc.
Phone: (307) 742-5555
support@handelit.com
www.handelit.com

Table of Contents

Section 1: Getting to the Administration Tree

When you log into RiteTrack®, if you are assigned as an Administrator for your RiteTrack® system, you will have an Admin tree. Most likely when you logged in, you will be looking at your "My Tree" which is the beginning screen for most RiteTrack® users. From there to access the Administration Tree, go to the upper left side of the screen where it says: "View: My Tree". From there, select the dropdown and select the "Admin" or "Administration" Tree.

Once you select it, you enter the Administrator view. In your navigation window you will have five different nodes. They are listed below:

1. Users
2. Security Groups
3. User Defined Lists
4. Organization Configuration
5. Lock Types

In the following sections we will describe each node and its function in your RiteTrack® System.

Section 2: What can you do from the Administration Tree?

Before we explain what each of the different nodes do and exactly how to navigate and change features of your RiteTrack® System, it is good to get a quick overview of what you are getting into and the ramifications of changes done to the Administrator Tree.

The Administration Tree allows you to manage the users of your system in a number of ways. You can limit what parts of the RiteTrack® System they can see, change and reset passwords, create or delete user groups and views, and change various items in your system as needed. It is said that with great power comes great responsibility, and that is true here as well. In the "My Tree" end user view of RiteTrack®, there is very little you can do to cause your RiteTrack® to stop functioning how you want it to. Here in the Administration view, that is much different. Some of the more complicated settings within the administrator tree should only be changed by a staff member of Handel Information Technologies. The more complicated settings will be mentioned within this document, but not explained in intricate detail.

As we move through this walkthrough, be observant for little ➡ icon. After this icon will be warnings about what could be done if you delete something. It is not meant to scare you but make you aware of what could happen. With that, we move on to the "Users" Node.

Section 3: The "Users" Node

3.1: Navigating Around

First we can navigate around the "Users" Node some so you get familiar. Just as in other parts of RiteTrack®, clicking the curved arrow will bring that item into your tree so you can look at it more closely. When you click on the "Users" Node, it will show all individuals who can log into your system. If you are on a new system, there should only be a few logins, one of those logins should be the one you are using. The list itself gives you limited information about each user, click on one of the users and bring them into your tree to see a more detailed view.

RiteTrack® auto-navigates to that user and shows you more information about that person. Here you can see the person's name, their role, if their account is enabled or not and if it is locked. You can also select the "Must Change Password" if you wish that user to be forced to change their password next time they login.

➡ ***WARNING***: If some of your users are using the web client, this checkbox should not be checked. This function is not available for those using the web client and as a result of checking that box, they will receive an error when logging into RiteTrack © that will not let them log in.

Once a login is created it is not recommended that you delete that user from the system or change the Person's name, but instead create a new login for that person and then uncheck the "Account Enabled" checkbox for the old user. The reason for this is because if that user was involved in key parts of the system, you will no longer have a history of what parts of the system that user took part in. Although it is not recommended to delete users, you still have the ability to remove them from the system. Adding new users will be covered farther down in this section, see Part 3.

➡ ***WARNING***: *Obviously deleting users is permanent and from that point on, until you recreate a login for them they will not have the ability access* RiteTrack® *at all. So, remember, if you are cleaning out old logins make sure you don't delete all the logins (Including your own!) or else you won't be able to access* RiteTrack® *at all!*

The Role field is where you can change what that person's primary function is in your system. To change it just select the dropdown and change it to whatever role he/she is now.

If "Account Enabled" is checked, RiteTrack® will recognize that the person you are editing is a current user. If it is unchecked, RiteTrack® will recognize that this user's login, although it still exists, is not a valid login and will not allow anyone to access the system with that User Name.

"Account Locked" allows you to lock out a certain login for a temporary or permanent basis. RiteTrack® will also automatically lock a login if there are a number of failed logins in a short period. If this happens to one of your users, you can come in here and uncheck that box and they will be allowed to log back in. The number of failed logins can be changed as you wish, feel free to contact Handel IT for information on how to do that.

In addition to the above, you have that user's unique login. This "User Name" can obviously be changed according to your own naming conventions. For the sake of organization, keeping the same naming conventions makes finding and editing users much easier.

The "New Password" and "Confirm Password" are blank. Even as an administrator you cannot see that person's password. What you can do is put in a new password, repeat the new password in the "Confirm Password" field, and click the "Reset Password" button. What this will do is set their password to the new one you typed in. This is helpful if you wish to login as that person to test something, but also guarantees that the user's chosen password is not known. As before, the "New Password" and "Confirm Password" fields become blank again as RiteTrack® encrypts the new password and secures it within the database. Last, you can assign an Organization to that individual. The organization is basically the primary Organization they are affiliated with.

3.2: More Complicated – "Groups" and "Tree Views"

Now that you are more familiar with what you are seeing, we can get more complicated. Click the (+) next to the user's name. The next two nodes are "Groups" and "Tree Views".

By clicking on the "Groups" node, it will show you all the security groups that this user is part of. The way RiteTrack® is setup, you can have one user be part of multiple security groups, allowing you to customize what each user sees without having to do too much work.

You can add, edit or remove groups from a user through this node. To add a group to a user, just click the "Add Group" button at the bottom of the screen. What is brought up are all of the “Security Groups” you have defined. Don’t have any? Don’t worry, we cover creating new “Security Groups” later on in this documentation. (See 3.3). RiteTrack® comes to you usually with your “Security Groups” already set up. Select one from the dropdown, make sure the “User” field shows the user you are working with, and click any of the checkboxes you want. If you wish it to be their Default “Security Group’ click Default. If you want them to inherit the predefined Group Trees, also click that. Once you are satisfied, click “OK” and it will add this Group to the user.

Now this person is part of the Group and will get all the permissions defined for that Group. If you don’t want a person part of a Group any longer, you can click on the red ‘X’. RiteTrack® will ask you if you wish to delete that Group, click “OK” and it is done.

> ➡ ***WARNING***: *Deleting all of the User Security Groups will leave that person with a login that has no permissions to anything. At least one User Security Group is required if you wish that person to be able to do anything in* RiteTrack®. *Please do not delete the Administrator security group. If this group is deleted, not even Handel will be able to log into your system. On a side note, if it is April Fools Day, it is a funny joke to do to them. But make sure to give them back their Security Groups after you are finished laughing and pointing.*

Now on to “Tree Views”, but what are Tree Views? Tree Views are groups of items that are required to navigate around RiteTrack®. For example if you take away the rt : Default : tool Tree View from someone, they will no longer be able to see their Toolbar. If you remove the rt : Default : nav Tree View, from a user, they will not have a Tree to navigate with. As an Administrator you can look at your own Tree Views, and not only will you see the default RiteTrack® views, those starting with ‘rt’, but also those starting with ‘admin’. Those admin Tree Views allows you to use the admin tree you are in right now. We could get into a discussion about the chicken and the egg, but worry not, if you work with RiteTrack® long enough, you will find the answer.

> ➡ ***WARNNG***: *Removing the ‘admin’ Tree Views from your own login will make it so you won’t be able to access them again once you log out.*

The following are the basic views for RiteTrack® and most likely you will only be working with:

admin : Default : nav = Access to the Admin Tree

admin : Default : menu = Access to the dropdown menus in the Admin Tree

admin : Default : Tool = Access to the Admin Tree toolbar

rt : Default : nav = Default Tree navigation for Rite RiteTrack® Track users

rt : Default : menu = Access to the dropdown menus in the default RiteTrack® user login

rt : Default : tool = Access to the toolbar in the default RiteTrack® user login

All the end users should have the rt : Default subset of Tree Views so they can work in RiteTrack®. As your system gets more complex, additional Tree Views may be added and assigned.

A quick way to add the default tree views to a new user, so that they can log into RiteTrack ©, is to right click on the "Tree Views" node. A popup menu will give you a few options. Click on the "Add Default Tree Views" option and then refresh your tree by pressing the F5 key on your keyboard. You will now see the added tree views in the right pane of your RiteTrack © screen.

3.3: Adding a New User to RiteTrack ©

Up to this point you are probably wondering how to add a user so a new person can use your RiteTrack® system. Up in the top left corner is a small person icon which when you mouse over it, says "New User…". Click on that button. A pop-up window very similar to the User Edit screen will come up. Fill out the information as needed. If you do not know if the person you are wishing to add is in the system, search the system using the regular RiteTrack® searching tool. If you do not find anyone satisfactory, you can then add a new person to the system. Once done, click "OK" and it will add that person as a user.

When you create a user he/she will not have any Groups or Tree Views. You will have to add them and design their security for that user as you wish. By adding them to Groups and adding Tree Views, you can fully customize their login to suit exactly what requirements are needed.

Section 4: The "Security Groups" Node

4.1: Navigating Around Security Groups

Just like the Users Node, the Security Groups Node is also setup the same way. When you first click on the node, a list of all the Security Groups already defined in your system will appear as a list on the right. You can then click on the curved arrow to add them to your Tree and that will allow you edit or delete that group. As you continue to move through the Administration Tree, this format will continue to show up and be familiar to you.

Add one of the Security Groups to your tree so you can see more information about it. Each Security Group should have a name that helps you understand what it does at a glance. Most Security Group information is self-explanatory. The "Active" Checkbox allows you to toggle on and off if that Security Group will be seen by RiteTrack® as active. The Priority allows you to set the Priority of securities compared to other Security Groups. This allows you to layer security so they can work together.

Now, expand a particular security group by clicking on the (+) symbol. Underneath you will see six nodes. This is a list of the nodes and a brief description of their functions:

View Permissions: View Permissions allow you to access or remove the ability to view certain parts of your RiteTrack® system. This permission can be adjusted to just be Ready only, all the way to full view permissions of Read/Write/Edit/Delete. A more detailed description is below. To add view permissions for specific forms, please contact a Handel IT representative, because only a trained staff member will know what the form's name is.

Entity Permissions: Entity Permissions allow you to what View Permissions do but on a larger scale. You can limit a Security Group so it cannot even see any cases at all, just people. Or you can limit a Security Group to only see certain Events in your process, but not all, depending on your needs. As of now Entity Permissions are left only for Handel IT staff.

Function Permissions: This allows you to give permissions to a Security Group that deals with activities a person can do in RiteTrack®. For example, if you don't want anyone of a certain group to be able to ever Re-Open a case, you can add a Function Permission and deny Permission to the "Allow Re-Open of Cases" function.

Policies: Policies are designed so that you can adjust how certain Security Groups view something in RiteTrack®. For example you can have one Security Group see text as the color Blue, while another the color Green, or you could even make it so one Security Group has a number of controls enabled, while another has only a few. This node works in conjunction with the Config tool and this is usually reserved only for Handel IT staff.

Tree Views: Because Tree Views are now set under the User, this node is currently disabled.

Lock Type Override: Here you can set an override for a Lock Type. For example, when an event is closed it locks so that nothing more can be done to it. You can set a certain Security Group to be able to override that Lock Type and edit a closed event.

> ➡ ***WARNNG***: *Because some of these admin functions work in conjunction with the Config Tool for* RiteTrack® *as well as the database, those reserved only for Handel IT staff should be left alone and requests for these kinds of changes should be sent to Handel IT.*

4.2: Adding a Security Group

Adding a Security Group is very similar to adding a User. Next to the "New User" button in the toolbar is a "New Security Group" button. Click that button and it will bring up a familiar pop-up. Fill in the information and click "OK" and that will create your new Security Group. Now you must "flush" out your Security Group to do exactly you want it to do by using the nodes provided.

If you left your Security Group as it is, anyone added to it would not have any view access or any other access to anything. The first thing you should do is add View Permissions to define what they can and cannot see. A good rule of thumb is to grant view access to everything then work your way down.

To do that, click the "Add Permission" button at the bottom. Proceed through each Object Type and give each Read/Write/Create/Delete permissions. For example, choose "Form" and under Object select "(Global)" and then click each checkbox. As you click the checkboxes you can see the Permissions number change. The number 15 means Read/Write/Create/Delete. This will give them global, or all of those items under that Object Type, permissions to all forms.

After you have set (Global) permissions to all of the different Object Types, you can start working down according to your wishes for that Security Group. For example, if you did not want a Security Group to see the Private Information form, you can bring up the "Add Permission" pop-up again, set the Object Type to Form, and then search the Object for that certain form. You can then set their permissions to None by leaving the checkboxes blank. The Permissions field should reflect that and have a 0 there. This may be difficult to work with for some customers because the names being used are the RiteTrack form names and not names you would be familiar with. Please contact Handel IT support for help with this until you are much more familiar with your system.

Section 5: The "User Defined Lists" Node

The "User Defined Lists" node is a list of all the items you as a customer wished us to put in RiteTrack® as custom information. This setup allows you to edit, change or delete items as you continue to use your system. This change will be reflected in your system the next time you logon, or when others logon to RiteTrack® after you made the change.

More often than not you will not be making changes here since, through configuration with Handel IT, these fields should be filled in as you wish it. If you feel uncomfortable changing things here, as always you can contact Handel IT at support@handelit.com to make changes for you.

Section 6: The "Organization Configuration"

The Organization Configuration node allows for you to create a kind of Security Group that relates to all individuals whose primary organization is the one listed. You can setup Entity Permissions and Policies that would work across the board despite individuals being part of different Security Groups. These kinds of security layers allow for much greater customization and more dynamic security. Because of the complex nature of Entity Security, this node is also reserved for Handel IT staff only.

Final Overview:

If you have gotten this far, you are a brave soul. The Administration Tree is not meant for the common End User. Fortunately, most of the functionality set here is done by Handel IT staff and more often than not you will have to deal with anything beyond Users and Security Groups, and those on a limited basis. As you spend more time looking through the Administration Tree and learning more about what you need in your system and how your system functions, maneuvering in the Administration Tree will get easier. As always if you are unsure about changes here in the Administration Tree, do not hesitate to call Handel Information Technologies, Inc. or email us at support@handelit.com. Also this documentation is meant for an overview to familiarize yourself with how the Administration Tree functions, and as you probably have surmised, parts of this Administration Tree are more complicated. Please use this documentation as a springboard into your training so you be prepared to ask questions on the more complicated issues.

Thank you!

Handel Information Technologies, Inc.